安徽科技学院处室函件

网络〔2018〕11号

关于印发《安徽科技学院网络与信息安全管理办法》的通知

各单位、各部门：

为加强对校园网络与信息安全工作的组织管理，提高网络信息安全防护能力和水平，明确管理责任，切实保障校园网络与信息安全，我们组织制定了《安徽科技学院网络与信息安全管理办法》，现印发实施。

特此通知。

网络与信息技术中心

2018年12月26日

安徽科技学院网络与信息技术中心　　2018年12月26日印发

安徽科技学院网络与信息安全管理办法

第一章 总则

第一条 为加强对网络与信息安全工作的组织管理，提高网络信息安全防护能力和水平，促进学校信息化建设的健康发展，根据相关法规和文件要求，结合学校实际，制定本办法。

第二条 学校网络与信息安全，是指由学校建设、运行、维护或管理的校园网、信息系统的安全，包括由学校各相关部门建设并负责维护管理的校园网络主辅节点设备、配套的网络线缆设施及网络服务器、网站、各管理信息系统、应用系统的安全等。

第三条 按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”的原则，建立健全网络信息安全责任体系。

第二章 管理体制和职责

第四条 学校网络安全与信息化领导小组负责全校网络安全体系与信息化建设的统一领导、统一谋划、统一部署，领导小组组长是学校网络信息安全的第一责任人，领导小组副组长协助组长履行学校网络信息安全责任。

第五条 各单位分管网络信息化工作的领导为本单位的网络与信息安全责任人，同时指定专人作为二级单位网络信息管理员，报网络与信息技术中心登记备案。二级单位网络信息管理员负责本单位网络信息安全保护措施的落实，负责对本单位上网人员进行网络信息安全教育和培训，与网络与信息技术中

心协作配合，共同做好本单位网络安全运行、管理和维护工作。

第六条 网络与信息技术中心是学校网络信息安全归口管理、技术服务支撑单位，负责学校网络与信息安全的建设、日常管理和维护，保障网络与信息系统的正常运行，负责落实有关网络与信息安全的法律法规，负责校内二级网络信息管理员进行网络信息安全教育培训和保密意识教育。

第七条 宣传部负责网站信息内容的安全审核、发布、监管，负责校园网络舆情信息的监控和管理，开展网上舆情疏导，同时负责对校内互联网群组和公众账号信息服务进行监管备案。

第八条 保卫处负责协助查处通过校园网进行的违纪、违法犯罪行为，对网络违规行为进行调查、取证、处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第九条 所有上网用户必须遵守《中国教育和科研计算机网络安全管理协议》等国家和上级主管单位制定的有关计算机连网和信息安全的法律法规，接受并配合国家和学校有关部门依法进行的对网络及信息系统的安全检查。

第三章 校园网络安全

第十条 校园网络是指连接学校各单位信息系统及信息终端的计算机网络，包括校园有线网络、无线网络和各种虚拟专网。

第十一条 校园网络与互联网及其他公共信息网络实行逻辑隔离，由网络与信息技术中心统一出口、统一管理，实名认

证。未经批准，各单位或个人在校园内不得擅自通过其他渠道接入互联网及其他公共信息网络。

第十二条 校内各类网络设备、设施、通信线路等，其管理、维护均由网络与信息技术中心统一负责，未经批准，任何人不得以任何方式试图登录、修改、设置、破坏校园网内的交换机、路由器和服务器等。

第十三条 网络与信息技术中心采取防火墙设置、身份认证、安全审计、MAC 地址绑定、病毒防护及入侵检测等安全技术手段加强校园网络边界防护。

第十四条 个人用户申请接入校园网络，须实行实名认证上网登记制度，并对上网认证帐号安全使用负责；公用账号的管理者应当加强对公用账号的管理，建立账号使用登记制度，确保公用账号合法使用。

第十五条 因科研、教学和管理需要须架设服务器的，必须以单位名义向网络与信息技术中心申请备案，严格限制服务范围，不得向其所在子网和校园网主干发送服务流量。禁止在校园网内私自架设服务器，对校园网用户或互联网提供网络服务。

第十六条 接入校园网的机房、电子阅览室等须根据相关法规建立用机管理规定，切实做好上机登记，并对上网行为进行有效监管。

第十七条 在校园网络上严禁下列行为：

（一） 破坏、盗用、篡改计算机网络中的信息资源；

（二） 故意泄露、窃取、篡改个人电子信息，擅自利用网络收集、使用个人电子信息，出售或者非法向他人提供个人电子信息；

（三） 违背他人意愿、冒用他人名义发布信息；

（四） 攻击、入侵、破坏计算机网络、信息系统及设备设施；

（五） 故意阻塞、中断校园网络，恶意占用网络资源；

（六） 故意制作、传播、使用计算机病毒、木马、恶意软件等破坏性程序；

（七） 故意大量发送垃圾电子邮件、垃圾短信等，干扰正常网络秩序；

（八） 盗用他人帐号、盗用他人 IP 地址；

（九） 私自转借、转让用户帐号造成危害；

（十）滥用网络，私自开设二级代理和路由接纳网络用户，私自改变校园网拓扑；

（十一） 上网信息审查不严，造成严重后果；

（十二） 以端口扫描和私搭 DHCP 服务器等方式，破坏网络正常运行；

（十三） 私自将互联网及其他公共信息网络接入校园网络；

（十四） 其它违反法律法规或危害网络与信息安全的行为。

第四章 信息系统及其数据安全

第十八条 学校域名为ahstu.edu.cn，各单位（部门）根据信息系统实际使用需求向网络与信息技术中心申请二级域名和服务器地址，经备案后开通使用。

第十九条 学校非涉密信息系统接入校园网络，应到网络与信息技术中心办理接入审批和备案登记手续。涉密信息系统不得接入校园网络。

第二十条 网络与信息系统的主办单位承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等职责。网络与信息系统的使用单位和个人对系统操作与信息内容的安全监管承担直接责任。网络与信息系统通过外包服务方式进行维护的，主办单位负责督促外包服务单位做好安全运维工作，网络与信息系统的安全监管责任主体仍为主办单位。

第二十一条 各单位（部门）原则上应依托校园网开展信息系统建设。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外。需要在校外开办信息系统的单位，应到网络与信息技术中心办理备案手续。部署在校外的网络和信息系统，安全监管责任主体仍为主办单位。

第二十二条 各单位（部门）对于主办的信息系统，应制订相应管理制度，建立健全信息发布、信息审查、应急处置机制，明确专门管理人员，采取必要的安全措施，严防入侵、篡改、泄露等事件发生。

第二十三条 各单位(部门)作为信息系统安全的责任主体，应当按照国家信息安全等级保护的管理规范、技术标准加强建设和管理，并配和网络管理部门做好等级保护相关工作。

第二十四条 各单位（部门）对于新建、改建、扩建的信息系统，应当在规划、设计阶段同步建设网络信息安全保障措施，使用符合国家有关规定、满足计算机信息系统安全保护需求的信息技术产品。

第二十五条 各单位（部门）应做好网络与信息安全事件的风险评估和隐患排查工作，制订完善相关应急预案，建立本单位信息安全值守制度，做到安全事件早发现、早报告、早控制、早解决，及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害。

第二十六条 各单位（部门）应建立检查巡查机制， 定期或不定期组织开展信息系统安全演练，查找安全漏洞和隐患。对机房、网络设备、服务器等设施定期开展安全检查。及时更新和升级必要的服务器软件，安装补丁，包括操作系统、web 服务器、应用中间件、数据库等，加强服务器应用的安全性。对上述检查中发现安全漏洞和隐患的，应当立即采取措施进行隔离，直至修复完成。

第二十七条 各单位（部门）对于主办的信息系统，每季度至少进行 1 次安全检查，检查内容包括：

（一） 查杀病毒，清除木马、后门等恶意程序，升级系统

补丁；防范网络入侵、攻击破坏等危害网络安全行为的措施；

（二） 检查重要数据管理、备份、容灾恢复措施情况；

（三） 检查网页内容，及时清除无关网页和暗链；

（四） 定期更改口令，清理不必要的管理账号；杜绝空口令、弱口令和默认口令；

（五） 检查SQL注入和跨站脚本等安全漏洞；

（六） 检查服务器安全策略，关闭不必要的端口和服务；

（七） 检查系统日志留存情况，留存相关日志不少于六个月。

第二十八条 各单位（部门）对于主办的重点信息系统，如学校门户网站、办公系统、统一身份认证、一卡通等校级重要公共服务平台，以及教务、学工、科研、人事、财务、资产等学校重要业务信息系统及相关重要数据库等应当采取措施重点防护，保障系统和重要数据的安全。

第二十九条 校园网用户应遵守国家有关法律、法规，严格执行安全保密制度，不得利用计算机国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动；不得利用计算机国际联网进行搜集、整理、窃取国家秘密的活动。

第三十条 任何单位和个人不得利用计算机网络从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机网络及信息系统的安全，不得利用校园网制作、复制、查阅和传播下列信息：

（一） 煽动抗拒、破坏宪法和国家法律、行政法规实施；

（二） 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一；

（三） 损害国家荣誉和利益；

（四） 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗习惯；

（五） 宣扬恐怖主义、邪教、封建迷信，违反国家宗教政策；

（六） 捏造或者歪曲事实，散布谣言，扰乱社会秩序，破坏社会稳定；

（七） 侮辱他人或者捏造事实诽谤他人；

（八） 含有淫秽、色情、赌博、暴力、欺诈等内容；

（九） 含有法律、法规禁止的其他内容。

第五章 应急报告与处置

第三十一条 学校网络安全与信息化领导小组统筹指挥网络与信息安全应急处置工作，负责建立健全学校网络与信息安全类突发事件应急工作机制，提高应对网络与信息安全类突发公共事件的能力，维护学校的安全稳定。

第三十二条 网络与信息技术中心根据《《安徽科技学院突发公共事件应急预案》（校发〔2016〕15号），做好安全事件应急处置，负责信息收集、分析和通报工作，按照规定向全校统一发布网络安全监测预警信息，并不定期组织全校范围内的

安全应急演练和安全培训。

第三十三条 各单位（部门）在应急事件发生时，按照应急处置预案处置程序，必要时可先断网，向单位主要负责人汇报，同时向学校网络安全与信息化领导小组或网络与信息技术中心汇报，获得技术支持，并及时报告处置工作进展情况，直至处置工作结束。

第六章 责任追究

第三十四条 学校网络安全与信息化领导小组对违反本办法的可根据情况作以下处理：

（一）警告、责令整改；

（二）关停网络 3 至 60 天；

（三）关闭端口、停止或限制服务；

（四）严重警告、通报所在单位，给予相应的处分；

（五）情节特别严重的，学校向公安部门报告，追究其法律责任。

第七章 附则

第三十五条 本办法由学校网络安全与信息化领导小组办公室（网络与信息技术中心）负责解释。